ZAP Scanning Report

Generated with ZAP on Wed 28 Aug 2024, at 17:08:44

ZAP Version: 2.15.0

ZAP is supported by the Crash Override Open Source Fellowship

Contents

About this report

Report parameters

Contexts

No contexts were selected, so all contexts were included by default.

Sites

The following sites were included:

- `http://zero.webappsecurity.com`

(If no sites were selected, all sites were included by default.)

An included site must also be within one of the included contexts for its data to be included in the report.

Risk levels

Included: `High`, `Medium`, `Low`, `Informational`

Excluded: None

Confidence levels

Included: `User Confirmed`, `High`, `Medium`, `Low`

Excluded: `User Confirmed`, `High`, `Medium`, `Low`, `False Positive`

Summaries

Alert counts by risk and confidence

This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	1 (100.0%)	0 (0.0%)	0 (0.0%)	1 (100.0%)
	Low	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Informational	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Total	0 (0.0%)	1 (100.0%)	0 (0.0%)	0 (0.0%)	1 (100%)

Alert counts by site and risk

This table shows, for each site for which one or more alerts were raised, the number of alerts raised at each risk level.

Alerts with a confidence level of "False Positive" have been excluded from these counts.

(The numbers in brackets are the number of alerts raised for the site at or above that risk level.)

		Risk			
		High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
Site	http://zero.webappsecurity.com	0 (0)	1 (1)	0 (1)	0 (1)

Alert counts by alert type

This table shows the number of alerts of each alert type, together with the alert type's risk level.

(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)

Alert type	Risk	Count
Hidden File Found	Medium	1 (100.0%)
Total		1

Alerts

Risk=Medium, Confidence=High (1)

http://zero.webappsecurity.com (1)

Hidden File Found (1)

▼ GET http://zero.webappsecurity.com/server-status

Alert tags

- OWASP_2021_A05
- OWASP_2017_A06
- CWE-538
- WSTG-v42-CONF-05

Alert description

A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.

Other info

apache_server_status

Request

▼ Request line and header section (271 bytes)

```
GET
http://zero.webappsecurity.com/server
-status HTTP/1.1
host: zero.webappsecurity.com
user-agent: Mozilla/5.0 (Windows NT
10.0; Win64; x64; rv:125.0)
Gecko/20100101 Firefox/125.0
pragma: no-cache
cache-control: no-cache
referer:
http://zero.webappsecurity.com/
```

▼ Request body (0 bytes)

Response

▼ Status line and header section (176 bytes)

```
HTTP/1.1 200 OK
Date: Wed, 28 Aug 2024 15:58:31 GMT
Server: Apache-Coyote/1.1
Access-Control-Allow-Origin: *
Content-Type: text/html;charset=UTF-8
Content-Length: 5523
```

▼ Response body (5523 bytes)

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD
HTML 3.2 Final//EN">
<html><head>
    <title>Apache Status</title>
</head><body>
<h1>Apache Server Status for
localhost</h1>

<dl><dt>Server Version:
Apache/2.2.22 (Win32) mod_ssl/2.2.22
OpenSSL/0.9.8t mod_jk/1.2.37</dt>
```

```
    <dt>Server Built: Jan 28 2012
11:16:39
    </dt></dl><hr /><dl>
    <dt>Current Time: Friday, 18-Jan-
2013 14:55:36 GMT</dt>
    <dt>Restart Time: Friday, 18-Jan-
2013 14:29:04 GMT</dt>
    <dt>Parent Server Generation:
0</dt>
    <dt>Server uptime:  26 minutes
31 seconds</dt>
    <dt>5 requests currently being
processed, 59 idle workers</dt>
</dl>
<pre>_____________________________________
____________________K_____KK_W__K__
.....................................
.........................
.....................................
.........................
.....................................
.........................
.....................................
.........................
.....................................
.........................
.....................................
.........................
.....................................
.........................
.....................................
.........................
.....................................
.........................
.....................................
.........................
.....................................
.........................
.....................................
.........................
.....................................
.........................
.....................................
.........................
.....................................
.........................
.....................................
```

```
.........................
.................................
.........................
.................................
.........................
.................................
.........................
.................................
.........................
.................................
.........................
.................................
.........................
.................................
.........................
.................................
.........................
.................................
.........................
.................................
.........................
.................................
.........................
.................................
.........................
</pre>
<p>Scoreboard Key:<br />
    "<b><code>_</code></b>" Waiting
for Connection,
    "<b><code>S</code></b>" Starting
up,
    "<b><code>R</code></b>" Reading
Request,<br />
    "<b><code>W</code></b>" Sending
Reply,
    "<b><code>K</code></b>"
Keepalive (read),
```

```
    "<b><code>D</code></b>" DNS
Lookup,<br />
    "<b><code>C</code></b>" Closing
connection,
    "<b><code>L</code></b>" Logging,
    "<b><code>G</code></b>"
Gracefully finishing,<br />
    "<b><code>I</code></b>" Idle
cleanup of worker,
    "<b><code>.</code></b>" Open
slot with no current process</p>
<p />
PID Key: <br />
<pre>
   11740 in state: _ ,   11740 in
state: _ ,   11740 in state: _
   11740 in state: _ ,   11740 in
state: _ ,   11740 in state: _
   11740 in state: _ ,   11740 in
state: _ ,   11740 in state: _
   11740 in state: _ ,   11740 in
state: _ ,   11740 in state: _
   11740 in state: _ ,   11740 in
state: _ ,   11740 in state: _
   11740 in state: _ ,   11740 in
state: _ ,   11740 in state: _
   11740 in state: _ ,   11740 in
state: _ ,   11740 in state: _
   11740 in state: _ ,   11740 in
state: _ ,   11740 in state: _
   11740 in state: _ ,   11740 in
state: _ ,   11740 in state: _
   11740 in state: _ ,   11740 in
state: _ ,   11740 in state: _
   11740 in state: _ ,   11740 in
state: _ ,   11740 in state: _
   11740 in state: _ ,   11740 in
state: _ ,   11740 in state: _
   11740 in state: _ ,   11740 in
state: _ ,   11740 in state: _
   11740 in state: _ ,   11740 in
state: _ ,   11740 in state: _
   11740 in state: _ ,   11740 in
```

```
state: _ ,   11740 in state: _
   11740 in state: _ ,   11740 in
state: _ ,   11740 in state: _
   11740 in state: _ ,   11740 in
state: K ,   11740 in state: _
   11740 in state: _ ,   11740 in
state: _ ,   11740 in state: _
   11740 in state: _ ,   11740 in
state: K ,   11740 in state: K
   11740 in state: _ ,   11740 in
state: W ,   11740 in state: _
   11740 in state: _ ,   11740 in
state: K ,   11740 in state: _
   11740 in state: _ ,
</pre>
<hr />To obtain a full report with
current status information you need
to use the <code>ExtendedStatus
On</code> directive.
<hr>
<table cellspacing=0 cellpadding=0>
    <tr><td bgcolor="#000000">
        <b><font color="#ffffff"
face="Arial,Helvetica">SSL/TLS
Session Cache Status:</font></b>
    </td></tr>
    <tr><td bgcolor="#ffffff">
        cache type: <b>SHMCB</b>,
shared memory: <b>512000</b> bytes,
current sessions: <b>0</b>
<br>subcaches: <b>32</b>, indexes
per subcache: <b>133</b><br>index
usage: <b>0%</b>, cache usage: <b>0%
</b><br>total sessions stored since
starting: <b>0</b><br>total sessions
expired since starting: <b>0</b>
<br>total (pre-expiry) sessions
scrolled out of the cache: <b>0</b>
<br>total retrieves since starting:
<b>0</b> hit, <b>0</b> miss<br>total
removes since starting: <b>0</b>
hit, <b>0</b> miss<br></td></tr>
```

	</table> </body></html>
Evidence	HTTP/1.1 200 OK
Solution	Consider whether or not the component is actually required in production, if it isn't then disable it. If it is then ensure access to it requires appropriate authentication and authorization, or limit exposure to internal systems or specific source IPs, etc.

Appendix

Alert types

This section contains additional information on the types of alerts in the report.

Hidden File Found

Source	raised by an active scanner (Hidden File Finder)
CWE ID	538
WASC ID	13

Reference

- https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html
- https://httpd.apache.org/docs/current/mod/mod_status.html